WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Industry Agenda

Partnering for Cyber Resilience

Towards the Quantification of Cyber Threats

In collaboration with Deloitte

January 2015

Contents

World Economic Forum®

REF 301214

Executive Summary

Threats grow with the rapid expansion of data-driven technologies. The convergence of web, cloud, social, mobile and Internet of Things platforms is inherently oriented to sharing data, not security. As these technologies expand in use, so do the risks, making cyber risk management imperative to organizations today.

Protecting against targeted threats without disrupting business innovation and growth is an increasingly critical business, economic and social imperative. Whether through lapses of trust, incompetence, or the application of new technologies and methods to perpetrate attacks, digital access assumes some level of risk. Completely eliminating cyber threats, including threats due to insiders or negligence, is not feasible. The World Economic Forum's Partnering for Cyber Resilience initiative revealed that cyber risk is increasingly viewed as a key component in enterprise risk management (ERM) frameworks.

The prevailing environment of uncertainty, along with accompanying pervasive risk aversion surrounding cyber threats, is restricting economic development. The spectre of potential threats hinders key digital ecosystem players from pursuing cyber-related commercial and public development initiatives. In 2014, the initiative focused on ways to model and quantify the impact and risk of cyber threats.

In the shifting environment of increasing interconnection, rapid technical development and evolving threats, a shared framework for cyber resilience assurance is required to support digital ecosystem decision-making at both macrosystemic and firm levels. A clear understanding of the risk environment – both residual (known and assumed) as well as evolving (unknown and uncovered) cyber risks – is necessary. Key factors include: internal "enterprise" versus external "systemic" risks; technical versus economic factors; and aligning enterprise cyber resilience maturity with insurance perspectives on risks.

For cyber resilience assurance to be effective, a concerted effort among ecosystem participants is required to develop and validate a shared, standardized cyber threat quantification framework that incorporates diverse but overlapping approaches to modelling cyber risk. A shared approach to modelling would increase confidence regarding organizational decisions to invest (for risk reduction), distribute, offload and/or retain cyber threat risks. Implicit is the notion that standardizing and quantifying such measures is a prerequisite for the desirable development and smooth operation of cyber risk transfer markets. Such developments require ERM frameworks to merge with insurance and financial valuation perspectives on cyber resilience metrics.

To pursue the goal of a shared cyber risk quantification approach, members of the initiative have framed the cyber value-at-risk concept. Envisioned to transcend traditional investment value at risk, cyber value-at-risk seeks to unify technical, behavioural and economic factors from both internal (enterprise) and external (systemic) perspectives. Understanding that organizations have different needs depending on factors such as the maturity of their security environment or the industry and sector they pertain to, the goal is not to provide a single model for quantifying risk. This report will identify key components towards a framework to cyber risk modelling and qualifying and quantifying known vulnerabilities in defenses, while providing macro-systemic guidance.

For organizations and industry stakeholders to be better positioned to make sound investment and risk mitigation decisions, they need to be able to quantify cyber risk. This can be achieved by a three-folded approach:

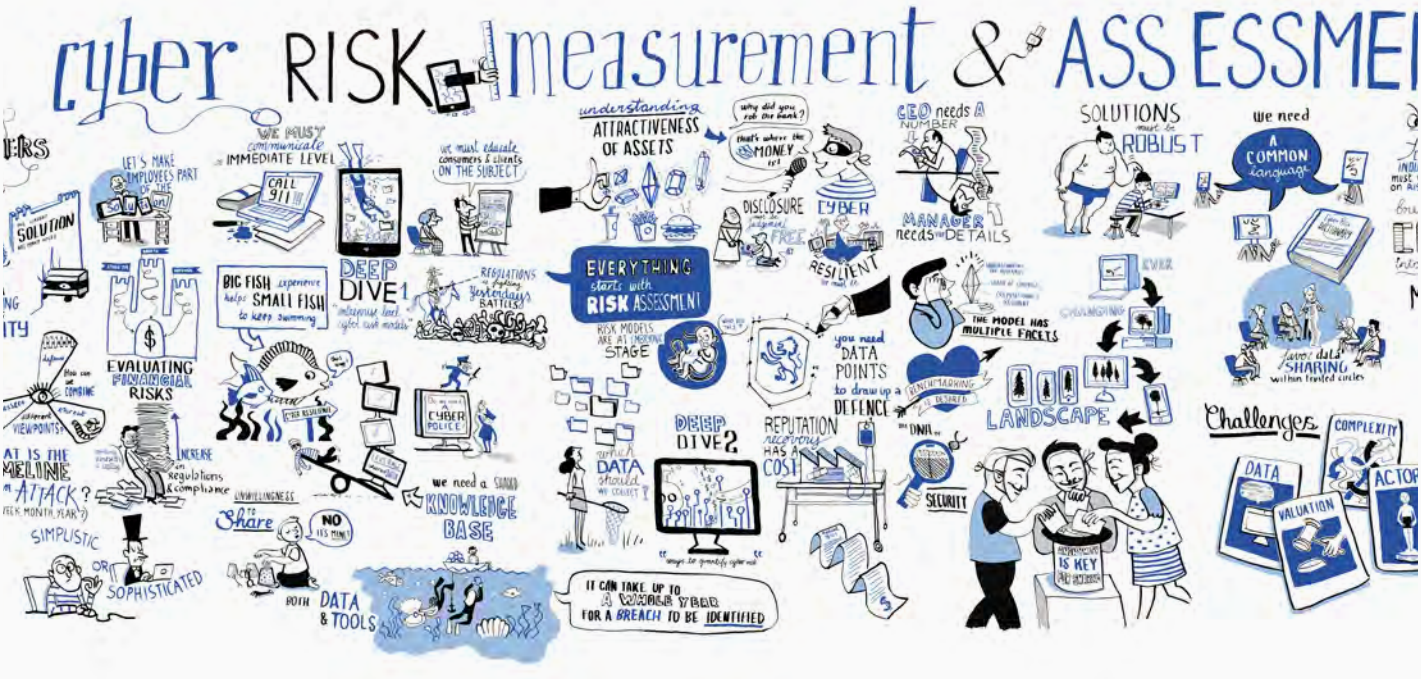
— Understand the key cyber risk drivers (or components) required for modelling cyber risks
— Understand the dependences between these components that can be embedded in a quantification model
— Understand ways to incorporate cyber risk quantification into enterprise risk management

While there is no ideal model that initiative members would unilaterally support, they encourage companies and industries to measure and work towards better quantification of cyber risks. The key components identified in the cyber value-at-risk model concept are:

— Existing vulnerabilities and defense maturity of an organization
— Value of the assets
— Profile of an attacker

This report summarizes the goals and activities of the initiative, the history and status of the initiative and key cyber value-at-risk concept foundations. It describes various possible components of the cyber value-at-risk framework, remaining challenges in moving towards more robust cyber risks quantification, and suggested next steps.

We would like to express our sincere gratitude to over 100 experts, business and policy leaders who have contributed to this work. Without their valuable contribution this project would not have been possible. We wish to thank our project advisor Deloitte, and in particular, Jacques Buith and Dana Spataru who have provided strategic advisory support for the project. Appreciation also goes to the core team at the World Economic Forum, Derek O'Halloran and Elena Kvochko for their leadership in this project.



Background

2011: Kick-off and context

From the outset, the core principles of the World Economic Forum's Partnering for Cyber Resilience initiative were established to raise awareness of cyber risk and to build commitment regarding the need for more rigorous approaches to cyber risk mitigation. The core principals are:

1. **Recognition of interdependence**
   All parties have a shared interest in fostering a common, resilient digital ecosystem

2. **Role of leadership**
   Encourage executive-level awareness and leadership of cyber risk management

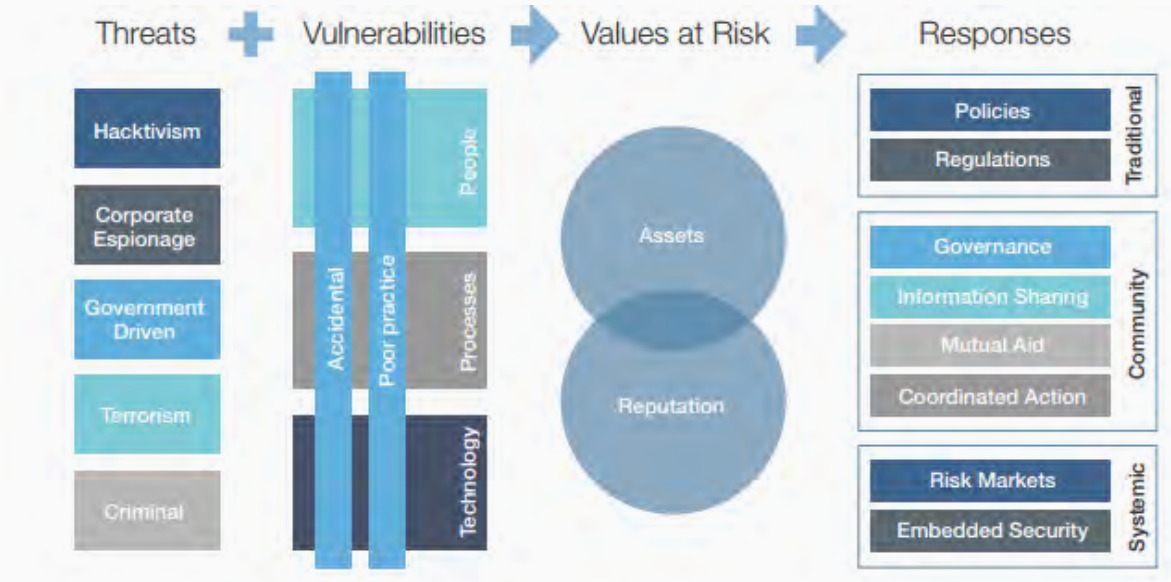
3. **Integrated risk management**
   Develop a practical and effective implementation programme that aligns with existing frameworks

4. **Promote uptake**
   Encourage suppliers and customers alike to develop similar levels of awareness and commitment

The initiative started at the World Economic Forum Annual Meeting 2011 in Davos when the Forum and its community of public and private sector organizations launched a multistakeholder project to address global systemic risks arising from the growing digital connectivity of people, processes and infrastructure (Internet of Things).

Early efforts focused on establishing context and tools for dialogue. A series of workshops organized around the Principles and Guidelines for Cyber Resilience advanced discussion to produce valuable guidelines and best practice principles for chief executives and government leaders. While the initial focus was on raising senior leader-level awareness of – and attention to – cyber resilience, the initiative has recognized the need for a shared cyber resilience assurance benchmark across industries and domains.

The following cyber risk framework was developed to improve cyber resilience of individual organizations, with critical components for organizations to consider, including existing threats, vulnerabilities, value-at-risk and potential responses.



2012: Building awareness

A summary of core principles and scope was published along with an assessment survey, *Partnering for Cyber Resilience: Risk and Responsibility in a Hyperconnected World – Principles and Guidelines*. in close collaboration with Deloitte, the initiative also produced a report summarizing feedback from the survey and related discussions entitled *Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience*.

2013: Issuing targeted guidance

The initiative presented a comprehensive set of options for increasing cyber resilience and for mitigating the economic and strategic impacts of global digital ecosystem cyber threats. The intent was threefold:

— Encourage awareness, understanding and action among top public and private sector leaders
— Assess cyber threat risks and associated economic impact
— Issue an informed set of recommended actions to mitigate the strategic and economic effects of threats through institutional readiness, policy development, critical infrastructure protection and information sharing

2014-2015: Proposing an assessment framework

The initiative, comprising more than 100 signatories, focused on ways to assess (model, measure and quantify) the impact of and exposure to cyber threats. Inputs were gathered from practitioners across a broad range of backgrounds and industries – industry leaders, vendors, regulators, public sector participants and other stakeholders. Building on the previous work and the cyber risk framework developed with the community, the initiative focused on identifying critical risks to the organizations and potential steps to cyber risk quantification models.

01: Francis Bouchard, Group Head of Government and Industry Affairs, Zurich Insurance, Andres Ruzo, CEO, Link America, Jan Verplancke, Director, Chief Information Officer and Group Head, Technology and Operations, Standard Chartered Bank, Thom Mason, Laboratory Director Oak Ridge National Lab, Brian Behlendorf, Preston McAfee, Chief Economist, Microsoft

02: Participants of a cyber risk measurement workshop
03: Patrick Jones, Senior Director, Stakeholder Engagement, ICANN

01: Participants of a cyber risk quantification session

02: Annemarie Zielstra, Director, Cyber Security and Resilience, TNO

Introduction

There are numerous cyber threats plaguing global organizations. Global data is expanding at exponential rates in terms of volume, velocity, variety and complexity. Commercial and personal data are increasingly migrating to global, interconnected technology platforms. The systems that depend upon this data increasingly manage key infrastructure. As access to data and systems increases via the rapidly evolving, interconnected digital ecosystem, the scale and types of risks from cyber threats expands proportionately.

Unknowns concerning the scale and impact of cyber threats, as well as relative levels of vulnerability, threatens paralysis. Lacking accepted benchmarks, large organizations struggle to structure cyber resilience decisions and investments. Organizations lack common measures to quantify cyber threats, curtailing the ability to make clear strategic decisions concerning optimal access and investment levels.

Due to this state of uncertainty, a pervasive concern over growing cyber risks curtails technical and economic development on a global scale. Lacking proper guidance, businesses are increasingly delaying the adoption of technological innovations due to inadequate understandings of required countermeasures. A tragedy of the commons scenario is emerging surrounding proliferating digital access in an unstable ecosystem, which lacks concerted controls and safeguards. A vicious circle results: uncertainty regarding proper levels of preparedness leads to forestalled investments in safeguards as interconnection expands exponentially.

Substantial actions are required from stakeholders across the shared digital ecosystem in order to address this systemic lack of resilience. A shared context for cyber resilience needs to be clarified for organizations to adapt to and counter continually evolving threats. This evolution can be supported through working towards a framework that, other than just permitting companies to advance their efforts to quantify cyber risk, allows for deep understanding of the underling risk sources, by evaluating the key drivers – referred to in this report as components – and hence provides insights about how to improve the current risk exposure.

Traditional cybersecurity tends to emphasize the type of attacker and the methods used in the attacks. A shift in business relevance and response effectiveness can come from adding a focus on asset (both digital and physical) and building cyber use cases at the intersection of all attacker, type of action (attacks) and assets at risk.

Since that can produce a very large list of use cases, the Forum initiative proposes to filter them using a model that rates both probability (risk) and impact (asset as specifically determined for an industry sector). The filtered results are the basis for a prioritized set of cyber use cases, and these can be further specified and built into the model for each specific industry.

Since no preferred models are available, companies are recommended to build their own stochastic models taking into consideration the above mentioned high-level components. In considering these components, it is essential that when scoping the investment in mitigating cyber risks, stakeholders should recognize that the enterprise must be secure, attentive to new risks and opportunities, and rapidly able to handle critical incidents. In addition, the security strategies must be built into the business strategy, the organization, the operations and the technology.

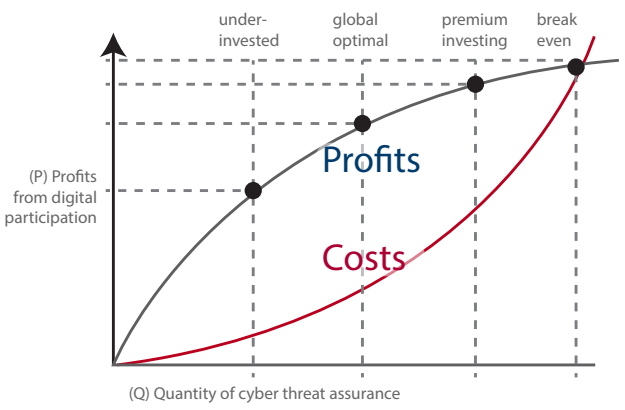
Cyber value-at-risk is characterized by generic applicability across industries, scalability, ease of interpretation and ability to support executive's investment and risk management decisions. Building the complete cyber value-at-risk model and having a comprehensive outlook on the organization's assets under threat, organizations can also make decisions with regard to the appropriate amounts of investments in security systems, as demonstrated in Figure 1.

The Partnering for Cyber Resilience initiative recognizes that, although desirable, the ability to calculate industry-wide measures presupposes standardization in cyber resilience metrics supported by comprehensive systemic tracking (e.g. via a commonly adopted threat index or systemic threat level tracked by a trusted third party or consortium of parties).

The cyber value-at-risk model helps answer the following cyberattack questions for stakeholders:

- **Who and why?** Addresses threat types executing the attack scenario in terms of target attractiveness (encompassing threat motivations and exposed target characteristics)
- **What and how?** Addresses the type of attacks applied (in terms of technical means and level of sophistication)
- **Where and when?** Addresses vulnerability as per a standard cyber resilience maturity level measure

Figure 1. Optimal cyber resilience investment



Cyber Value-At-Risk Foundations

Models used for cyber threats assessment

Between August and November 2014, the initiative's core team convened four cyber risk measurement working group sessions. The sessions focused on assessing various existing methods for measuring and quantifying cyber threats.

An early challenge recognized by the working group was the great variety and diversity of ERM cyber resilience maturity models. Although ERM models bear similarities, they lack a unifying framework allowing transparent one-to-one translation. The resulting inability to track and assess systemic and relative residual risks raises the need for standardization.

Members of the initiative listed various types of models used within their companies. While the Monte Carlo method was predominant, elements of other models were determined necessary for a successful risk quantification model. The list included other techniques and methods such as parametric, behavioural modelling, baseline protection model, the Delphi method and certifications.

Monte Carlo Method – Is a problem-solving technique used to estimate the probability of certain outcomes by running trial runs, called simulations, using random variables. A Monte Carlo simulation allows an analyst to quantify the uncertainty in an expert's estimate by defining it as a probability distribution rather than just a single expected value.

Behavioural Modelling – Is a technique which stresses the importance of human behaviour when designing, building and using cybersecurity processes. It builds on illustrating how behavioural science offers the potential for significant increases in the effectiveness of cybersecurity.

Parametric Modelling – Uses parameters to define a model. In statistics, a parametric model is a family of distributions that can be described using a finite number of parameters.

Baseline Protection – Centres on achieving an adequate and appropriate level of security for IT systems. It is a methodology used to identify and implement computer security measures in an organization.

Delphi Method – A forecasting or decision-making technique that is used to add predictive analysis.

Certifications – Can be used as a means to complying with security standards, as well as global and local rules and regulations. These guides offer general frameworks as well as specific techniques for implementing cybersecurity.

Although originating in various industries such as insurance, technology or cyber consulting, it was agreed that the various cyber risk models reviewed had more similarities than differences. This was considered a positive indication in the effort to establish a unified, shared model.

Feedback was gathered concerning key desirable attributes for a shared model. The attributes include:

Applicability
Ability to apply the model across different industries, organizations and adjust it depending on the needs of the company
- Generic applicability across industries
- Scalable to address differing level of maturity
- Suitable for customization
- Ease of interpretation
- Traceable and transparent

Precision
Comprehensiveness and measurement accuracy of the model
- Balances generalizability, accuracy and precision
- Practical concerning data availability

Timeliness
Ability to timely reflect the environment around incidents
- Ability to track previous incidents/cyber events
- Timely in tracking present and emerging risks

Scope
Ability to cover a wide range of factors and risks
- Provides for a market valuation of risk
- Complete in addressing internal and external risks
- Addresses both tangible and intangible risks

Decision-making process
Potential to serve as an effective risk measurement tool for executives and decision-makers
- Assists in supporting investment decisions
- Focuses on preserving value in the face of pervasive threats
- Compatible with existing enterprise risk management frameworks
- Establishes a foundation for cyber risk transfer markets and instruments

While the Initiative identified more similarities than differences among cyber risk models, a number of challenges were also identified. They include:
- Data availability and standardization, specifically concerning historical data on threats and breaches (in most industries there is no common information sharing standards or platforms, outside of financial services industry)
- Damage valuation standardization, including tangible and intangible assets, i.e. reputation and brand (measuring of the effects of cyber incidents against those assets is not standardized)
- Willingness to share information across companies (companies are unwilling to share information due to reputational and regulatory risks and due to the risks of misuse of information)

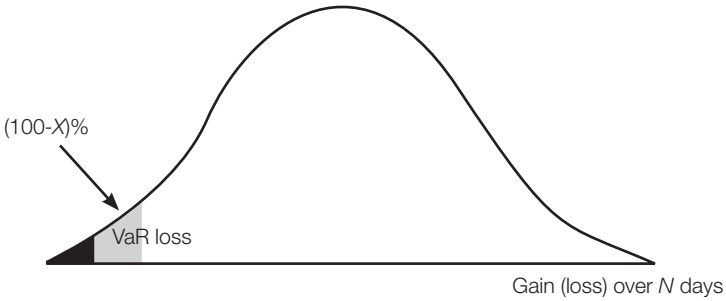
— Information asymmetry due to limited visibility into a company's cyber resilience (various executive functions within an organization have a different outlook on the maturity of their company in terms of security posture
— Matching between actual risks versus measured risks (the need for less error-prone models for assessing security posture)
— "Chicken and egg" challenge of risk transfer markets both requiring and justifying quantification efforts (insurance companies would like to offer competitive market solutions to offset cyber risks, but they do not have the necessary data to build these solutions; they do not have the data because they do not have ways of collecting it, e.g. by offering products in exchange for data).

What is cyber value-at-risk?

Just as commuting to work involves a small but statistically measurable risk of bodily harm, participating in the interconnected digital ecosystem involves adopting inherent residual and system risks. Another metaphor, even the most thorough medical diagnostic test certifying good health cannot guarantee against the future risk of disease. In an increasingly interconnected digital ecosystem, even well-guarded participants face the threat of a cyberattack. Beyond malicious hackers, cyber threats also encompass insider threats, breakdowns in trust, and faults due to negligence or ignorance. The uncertainty of risk can be quantified probabilistically given concerted attempts to track systemic metrics, be they the risk of an auto accident, susceptibility to cancer, or the risk of a cyber-incident given a particular cyber resilience profile.

The concept of cyber value-at-risk is based on the notion of value at risk, widely used in the financial services industry. In finance, VaR is a risk measure for a given portfolio and time horizon defined as a threshold loss value. Specifically given a probability X, VaR expresses the threshold value such that the probability of the loss exceeding the VaR value is X. In figure 2, the curve is the normal distribution of the risk, N days is the time horizon, the X axis is the performance of the portfolio and X represents the VaR threshold. (100 – X)% is the probability of not exceeding the VaR value

Figure 2. VaR curve



It is important to note that in this report we specify properties that VaR should have, but not specifically how to compute it. Cyber value-at-risk could be successfully applied to cyber risks as a proxy concept for risk exposure and could appeal to a wide range of industries and enterprises. This cyber risk model uses the probabilistic approach to estimate the likely loss from cyberattacks over a given period.

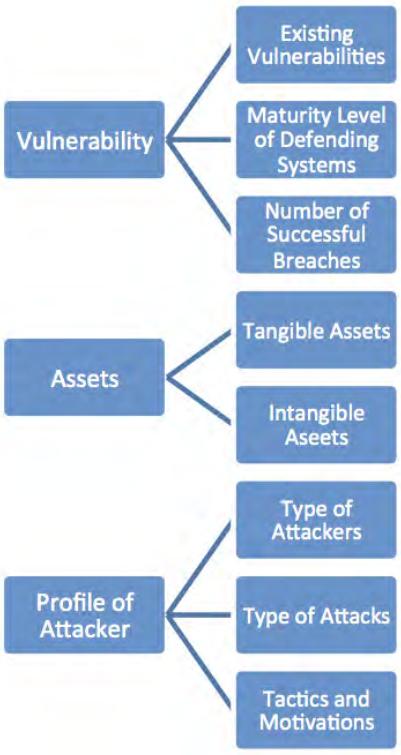
Cyber value-at-risk requires organizations to understand the key cyber risk drivers (or components) required for modelling cyber risks, and the dependencies between these components which can be embedded in a quantification model. As an outcome, a complete and complex cyber value-at-risk model will help organizations answer address the following:

Given a successful cyberattack, a company will lose not more than X amount of money over period of time with 95% accuracy.

Cyber value-at-risk incorporates multiple components that need to be assessed by each organization in the process of cyber risk modelling. The applicability and impact in each model of these components will vary per industry and cyber resilience maturity. It is critical to analyse dependencies between the components of the model, as this should be embedded in the cyber risks quantification model.

The goal of cyber value-at-risk is to standardize and unify different factors into a single normal distribution that can quantify the value at risk in case of a cyberattack. The effort should both be specific to the organization and reflect industry-wide trends. Once there is a statistical model to measure cyber risks, it can be incorporated into a broader risk strategy of a company.

Figure 3. Cyber value-at-risk components



Component 1: Vulnerability
There are the potentially less protected assets and systems that can become target of the attacks

- *Existing vulnerability:* Number of unpatched vulnerabilities, ratio of newly discovered vulnerabilities per each product used in the network, success rate of compromises per each machine during internal and external assessments
- *Maturity level of defending systems:* Number of security updates, number of defensive software components installed in the network, number of previous compromises, network typology and infrastructure

Component 2: Assets
At the core of cyber value-at-risk is high-level identification of assets under threat. This varies by organization, but typically includes tangible assets (e.g. funds and financial instruments, infrastructure, and production capabilities) as well as intangible assets (e.g. knowledge, privacy data, reputation, trust, brand, etc.) and structure assets (e.g. processes or systems that could get disrupted)

- *Tangible:* Costs of temporary of business interruption, complete business interruption, regulatory fees
- *Intangible assets:* Costs of temporary of business interruption, complete business interruption, lost IP, reputation loss

Component 3: Profile of attacker
The profile of adversaries targeting valuable assets

- *Type of attackers:* State-sponsored vs amateur, sophistication level of attackers (not so sophisticated, sophisticated, very sophisticated)
- *Tactics and motivation*: Number of novel attacks used, tends to be destructive (yes/no), tends to steal information (yes/no)

The components, some of which can be represented by both random variables (a variable subject to change due to chance, such as frequency of attacks, general security trends, maturity of security systems in the organization, etc.) are put into a stochastic model (a statistical tool to estimate probability distribution, which has one or more random variables over a period of time). The statistical process will yield a probability distribution.

Companies that can analyse the dependencies between components can help various risk models estimate risk exposure. For example, the number of attacks a company or institution will experience depends on the assets and general trends or pattern in the attacker community. Therefore, assets (component 2) and profile of attacker (component 3) determine the attractiveness of the company in the face of global trends and data about cyberattacks. The combination of the two components can be used to quantify the entity loss of a successful attack. It is based on the hacker type executing the attack, the kind of attack used by the hacker and the maturity level of the victim's security system.

The success of an attack is determined by the interaction of the attacker with the victim's vulnerabilities in their security system. Profile of attacker (component 3) identifies hacker types and relative behaviour while the vulnerability (component 1) quantifies the maturity level of the defending system. The interaction between these two components leads to determining attack success rate.

Since the cyberattack phenomenon can be considered broadly as criminal, and thus social/behavioural and economic, understanding incentives, drivers and methods are critical to understanding the relative attractiveness of particular targets, and thus the relative likelihood of incidents. The behaviour of cyberattackers is influenced by the perceived "attractiveness" of an organization and may influence the particular methods and vigour applied to an attack. Although not all cyberattackers are motivated purely by financial gain, the decision to attack can be said to be economic in terms of assessing potential risks and rewards.

For example, linking patterns between standard cyber resilience maturity measures and "demographics" exposes hidden characteristics that predispose organizations to risk. In 2013, the Ponemon Institute's *Cost of Data Breach* study suggested a higher propensity for cyberattack losses can be attributed to companies with higher customer churn. Such useful indications, linking organizational factors to higher threat levels of attack, can only be achieved by expanding efforts to standardize, centralize and track metrics associated with digital participants and known incidents. Board members and senior management need risk-based metrics to quantify, mitigate and manage residual risk.

The components described above in the cyber value-at-risk concept provide the ability to quantify aggregate, pervasive risks in local terms, namely via measures of risk likelihood and impact. However, to achieve this level of specification, cyber risk standardization and quantification must first advance.

Mapping to enterprise risk management frameworks

With standardization and tracking of metrics, a cyber-technical resilience maturity profile could be mapped probabilistically into the ERM frameworks to known attack types. Traditional ERM measures of cyber risk typically do not quantify severity of financial loss in the event of a cyber incident. A focus on developing a framework to understand desirable and optimal investment levels and benchmarks for cyber resilience – given a particular risk appetite – would help to specify optimal levels of cyber resilience investment. Implicit is the notion that a discrete point of economic optimality exists between the benefits of digital access and the constraints of risks assumed.

Linking to financial service and insurance industry concepts of systemic risk would address such a gap. The financial service industry has used sophisticated quantitative modelling for the past three decades and has a great deal of experience in achieving accurate and reliable risk quantification estimates. To quantify cyber resilience, stakeholders should learn from and adopt such approaches in order to increase awareness and reliability of cyber threat measurements. A potential option, for instance, is to link corporate enterprise risk management models to perspectives and methods for valuing and quantifying "probability of loss" common to capital adequacy assessment exercises in the financial services industry (e.g. Solvency II, Basel III), albeit customized to recognize cyber resilience as a distinct phenomenon.

Quantifying assets with significant losses

As with other types of risks, the concern is not only with expected losses from cyber threats, but should incorporate an understanding of potential significant losses that could occur with a small but reasonable probability. Cyber value-at-risk can be thought of as the value exposed given both common and significant attack risks. Technically, financial value at risk is defined as the maximum loss for a given confidence interval (say, with 95% certainty) on a given time horizon (say within a year) in normal distribution. To capture these occurrences, extensive data sets are needed to capture rare events and fat-tail characteristics of the distributions, which are largely not available today (see the section of "availability of data" on addressing this challenge).

Practical example

Consider a company involved in the oil and gas industry. The first step to evaluate their risk should be to quantify the type of assets (component 2). It is important to reduce the scope to assets that are affected by a potential cyberattack. In this case, it is very likely that at least four types of assets will be involved:

1) The commodity (gas or oil)
2) The SCADA systems that control the industrial equipment
3) The industrial equipment itself
4) The organization's reputation

For all of the above assets, the risk is in terms of future revenue loss because of interruption, malfunctioning, destruction of the asset as well as government fines, litigation and PR costs. The company could estimate that the full interruption of production for a business day would result in a cost of $1 million split between the cost of unrealized revenue and the reputational damage. Moreover, the company can estimate that the full interruption of production for X days would cause the company to file for bankruptcy.

The second factor to consider is the attacker (component 3) in terms of motivation, resources and capabilities. This part of the assessment should use industry-wide historical data to measure the likelihood of the various potential actors to attempt an attack. Note that this data is imprecise by definition – not only because attribution in the cyberspace is a hard problem, but also because the nature of the attacker as well as the resources, capabilities and motivations change over time. Nonetheless, it is conceivable to expect that certain industries are more likely to be targeted by certain families of attackers compared to others.

For example, historical data might tell us that in the oil and gas industry 90% of the attacks are just temporary business interruptions perpetrated by hacktivists and 10% are permanent destruction of certain assets perpetrated by competitors.

Finally, the company security posture or vulnerability (component 1) should be evaluated. This implies evaluating a number of factors, such as:

— Number of known unpatched vulnerabilities
— Frequency of historical successful attacks
— Evaluation of the overall security made both by internal and external red-teams
— Other non-technical capabilities or the organization that contribute to its resilience (board-level awareness, availability of contingency plans, etc.)

In the ideal scenario, industry-wide scales/indices would be available. In that case, each company could be compared to the others in the same sector and this would give them the ability to correlate their security posture with the likelihood of an attack. In absence of such indices the company could run statistical simulations based on factors listed above and produce a statistical distribution representing the probability of a successful attack.

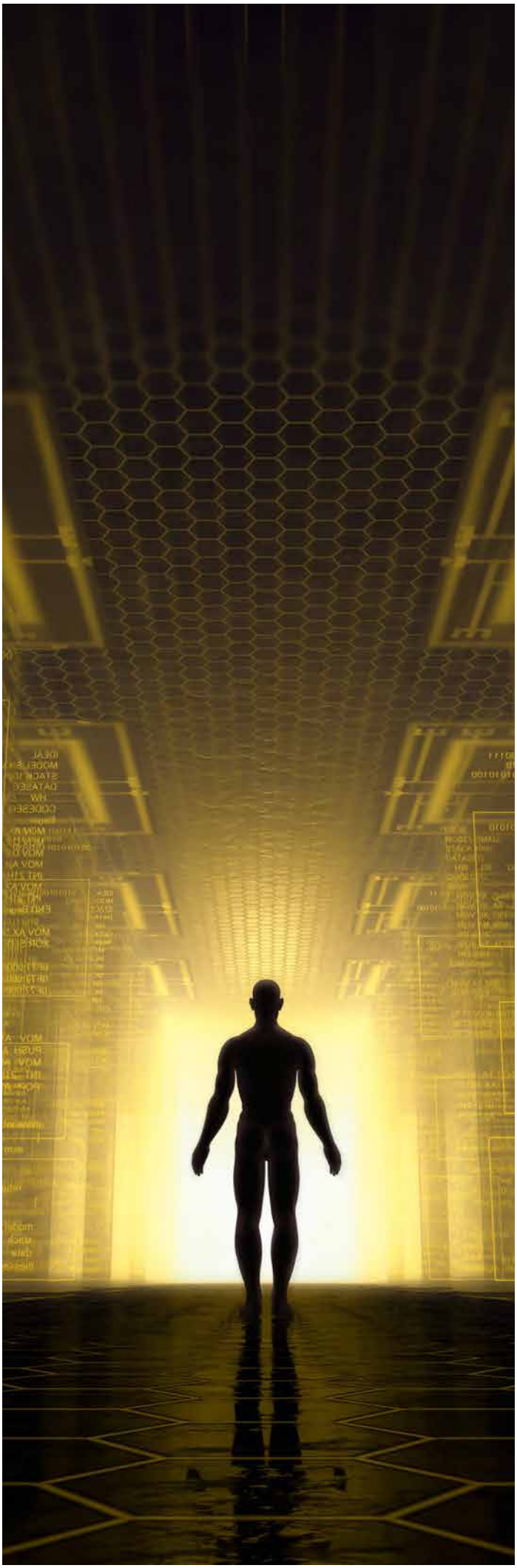
Calculating risk

As discussed, from a mathematical standpoint, the above variables can be combined together to form a stochastic model. This stochastic model best represents the cyber value-at-risk and its output is the probability on any given day to lose a certain dollar amount.

For example, for the fictional company mention above, the model could say that there is a 5% probability of losing $10 million on any given business day. The model would be run periodically to account for improvement to the security posture, change in risk profile and change in the attacker's behaviour.

One common problem faced in the cybersecurity industry is the lack of historical data. This shortcoming could potentially be addressed by running statistical simulations (i.e. Monte Carlo simulation) on the various random variables. The simulation will be reinforced by new data coming from known breaches as well as assessments of the company's security posture produced by internal and external red-teams.

From the examples above, there are key components that are necessary to consider and take into account when considering your risk exposure.



Addressing Cyber Value-At-Risk Limitations

Availability of data

One challenge with the cyber value-at-risk model pointed out by participants is the ability to estimate probabilities of a successful attack. The standard approach to quantify the hazard is first to assume probability distributions, both concerning the frequency and the severity of the risk events, and, secondly, to calibrate the distribution parameters to real data. Extensive data sets are needed to capture event occurrences.

Since extensive historical data is not available, reliable cyber risk data is a limitation due mainly to delays between events occurrences and their detection or manifestation, low or absent risk awareness by the subject of the attack and complex dependencies between event types. To overcome this problem the Initiative intends to use the cyber value-at-risk framework to identify the components, which need to be modelled as part of the risk process from its generation up to its realization and concretization. As an outcome of the initiative meetings, it was suggested that near real-time information sharing can address data availability challenges and supply enough data to build statistical models.

Availability of standardized maturity frameworks

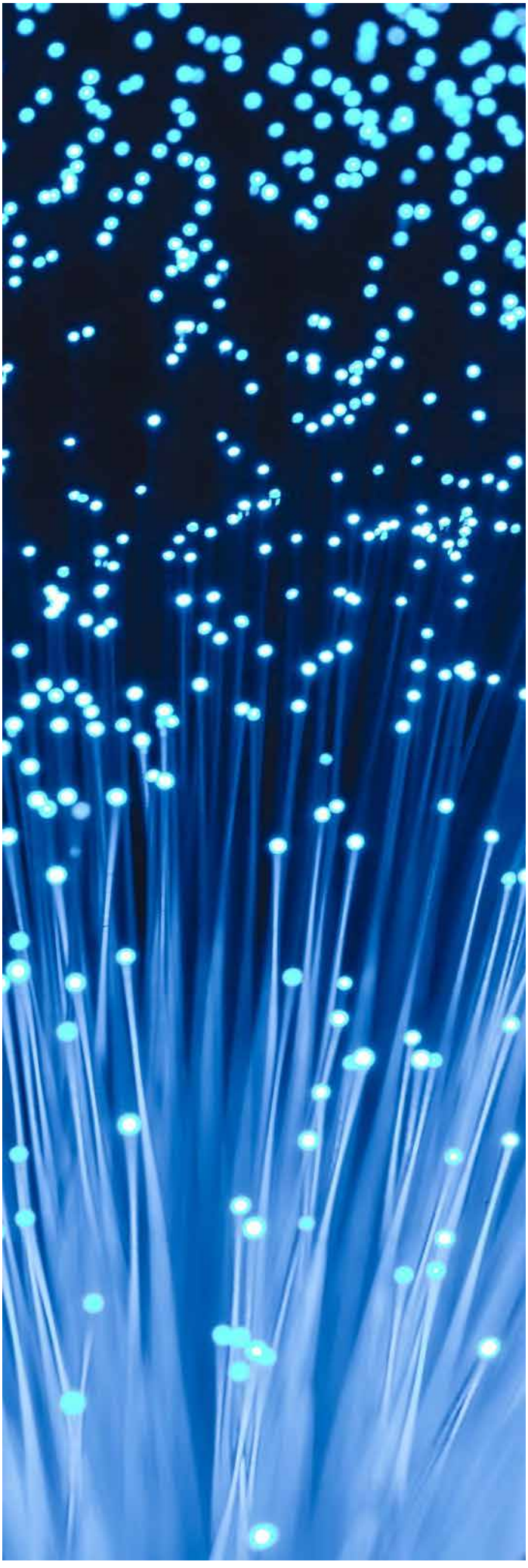
The number of incidents a company or institution will experience depends on the company's relative cyber resilience maturity. Standardized maturity measures would allow for a quantification of threat "attractiveness" and inherent vulnerabilities. To quantify threat attractiveness, companies need to adopt a standardized maturity model and a linked threat index.

The interaction between threat and threatened can be assessed as a probabilistic assessment of attack success rates per "attracted" threats (much as in an epidemiological model of relative health and exposure to disease risk factors). The discrete probabilities could be quantified, for instance, via a simulation (e.g. Monte Carlo or discrete event addressing the above mentioned challenges in a comprehensive way that takes into account the key components (see Figure 3).

Mitigation strategies

Having mitigation systems in place to address the key components in the model will help decrease the likelihood of an attack. Important mitigation strategies should include a proactive security system (unified combination of people, systems and processes to monitor, alert and respond comprehensively to a range of cyber threats), along with monitoring, detecting and responding capabilities.

- **Monitoring**, which involves verifying that the aggregate system (digital infrastructure) is functioning in an expected way
- **Detecting**, which involves spawning alerts concerning irregularities
- **Responding**, which involves counteracting any perceived threats by directly action intended to contain and control the threat (e.g. denying access to an account or IP address, taking a system off-line, or implementing active counter-measures such as a virus inoculation)



Path Forward

There is no silver bullet to address foolproof cyber resilience. Managing cyber risks requires a framework for segmenting and quantifying shared risk factors. Among the dimensions of an effective cyber risk model is quantification of assets, knowing the attacker profile and knowing the potential vulnerabilities of a company. Successful cyber risk includes organizational leadership, cyber life-cycle process management, and solution life-cycle implementation management.

Tracking discrete risk factors (i.e. via an accepted index) and establishing a shared cyber resilience maturity model will support enhanced leadership from the top and clear systemic digital ecosystem accountability. Organizations recognize that continued global systemic interconnection and technical development will continue and they should work to ensure that concerns surrounding the cyber risk ecosystem will be dealt with. Moreover, novel, emerging threats will put increasing pressure on key stakeholders to formulate a systemic, rather than patchwork response.

The biggest challenge with the cyber risk quantification models so far is not the technique chosen for modelling the risk, but rather the quality of the input variables. The type, precision and optimization of the risk model inside the cyber value-at-risk concept are relevant, but the input variables offered to the value-at-risk model are the main concern and should be addressed first.

Prior to discussing all variants of the most accurate and optimal model for quantifying risk, it is highly important that companies structure and standardize the input variables, or the components of the model. This will have a much bigger impact on the relevance and accuracy of the output of the model than fine-tuning the model type and detailed parameterization and configuration of the model.

In the same way in which a mature industry such as the car insurance industry has homogenized on an industry standard set of input variables, the growing cyber security industry should do the same. The car insurance industry standardized and benchmarked input variables, which are common practice for all car insurance companies: age, gender, claim history, number of years of no claim, weight of the car, year of built of the car and much more.

This homogeneous set even supports transferring insurances from one insurance company to another. They recognize and approve each other's input variables automatically without any discussion simply because the risk judgment is based on the same industry best practice set of standardized variables. Similarly, a standardized set of best practice input variables for cyber security risk modelling would help the cyber security industry tremendously in its effort to define the unified and standardized cyber security risk quantification models.

The brainstorming, gathering, categorizing and understanding the interdependencies between these input variables or components should be at the top of all cyber security meeting agendas. Most industries and companies do not have the needed data available to populate the input

variables. Only if the data sets, per component, are gathered structurally they can be used as reliable input variables for the cyber value-at-risk framework and support an accurate cyber quantification model. If these strong prerequisites have not been delivered and agreed upon, engaging in a cyber-risk quantification model design, optimization, configuration or accuracy is premature.

With the establishment of a common framework for quantifying cyber threats, comprehensive tracking of incidents and emerging risks can be engaged. Benefits would accrue in the ability to measure risk factors and potential damage at a more granular level. With trusted quantification measures in place, a greater range of market-based risk transfer and offload solutions will arise. For instance, taking the example of the carbon-credit trading market, intended to reduce global CO_2 emission burdens, the establishment of a shared cyber resilience threat index, along with a linked firm-focused cyber resilience maturity measure, would present the opportunity for a tradable "cyber resilience credits" market to arise.

Cyber threat options markets, collateralization of packaged cyber risks and insurance default swaps could be envisioned. However, such mature, functioning market infrastructure and instruments assumes commonly accepted cyber resilience maturity assessment "certification scores" for organizations. A cyber threat index or indices would be required to improve ongoing and emerging threat tracking, improving efficient information transparency based on the wisdom of crowds principle.

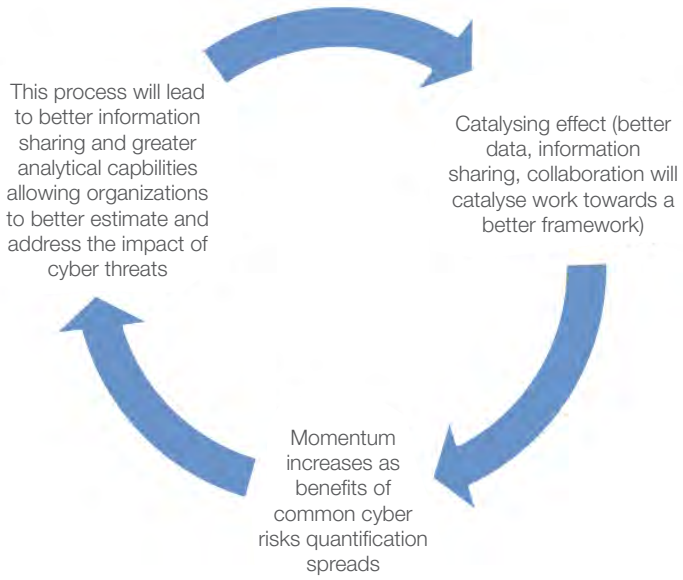
Standardization of threat level measures and assessments of firm vulnerability would empower both insurance providers and financial service players to offer a range of products and instruments for cyber risk transfer and alienability. This in turn would foster development of secondary risk instrument markets, such as collateralized cyber risk coverage dedicated to apportioning risk among smaller firms, options markets tied to cyber risk threat indices, and the potential for a market in cyber risk liability swaps to undergird the reinsurance market. The challenges present in this market that prevent effective risk transfer market formation include perverse incentives, moral hazard, potential for fraud and market manipulation, bubbles and market correlation. Such aspects suggest the involvement of government leaders and regulators in the establishment and monitoring of such markets.

An effective cybersecurity programme requires continuous and proactive engagement from senior management. In the first instance, promoting a cyber culture requires a cybersecurity tone from the top, including awareness and responsibility, defining the importance of cybersecurity as a corporate priority, and establishing clear governance, policy and oversight. A second consideration for management is the clear delineation of responsibilities and accountability for cybersecurity programmes, setting expectations and accountability of management and assuring the adequacy of resources, funding and focus. Overseeing the cybersecurity activities can be done through periodic cybersecurity risk reviews, regulatory compliance requirements, and metrics and reporting structure to filter critical risks.

As likelihood, impact and vulnerability around cyber threat risk could be potentially high, company boards have good reason to ask, "How likely is it to happen to us? What are we doing about it?" More broadly, the central issues for boards to consider are exposure and effectiveness. "What is our company's level of exposure to cyber threat risk? And how effective is the company at managing exposure within acceptable limits?"

Effective cyber risk management needs a board that guides/challenges management on the adequacy of cyber risk management practices, particularly around risk appetite and cyber security strategy. As such, further specifying and promoting cyber value-at-risk as a vehicle for global cyber resilience sustainability via functioning cyber risk transfer markets would benefit organizations and global stakeholders and support the creation of a more resilient cyber ecosystem.

Figure 4. Virtuous circle of cyber quantification



Acknowledgements

The team is grateful to our partner companies, contributors and members of the project working group for their thought-leadership and continuos engagement

Aaron Boyd	Chief Strategy Officer	ABI Research
Kathryn Kun	Adversarial Resilience	Akamai Technologies
Mark Armitage	Director, Security Management	Akamai Technologies
Stephen Cross	Chief Innovation Officer	Aon Plc
Arabella Whiting	Head, Cyber Security Strategy	BAE Systems
Vincenzo Iozzo	Member of Board	BlackHat Security conference
Adrian Turner	Managing Director	Borondi Group
Robert Rose	Senior Advisor to Chairman	Bridgewater Associates
Malcom Stokes	Head of Operational Risk - BT Security	BT Group
Claude Boudrias	Director, Government Relations	CA Technologies
Vikas Krishna	Products, Mobile Content, App & Email Management Solutions	CA Technologies
William Saito	Special Advisor	Cabinet Office of Japan
Simon Gibson	Head of Security (formerly: CTO at Bloomberg)	CCG LLC
Sameer Bhalotra	Strategic Technologies Program	Center for Strategic and International Studies
Kah Kin Ho	Head of Cyber Security Business	Cisco
Merit Janow	Dean, School of International and Public Affairs	Columbia University
Jane Holl Lute	Chief Executive Officer	Council on Cyber Security
Dmitri Alperovitch	Co-Founder, Chief Technology Officer	Crowdstrike
Jeff Moss	Founder	Defcon
Alan Murray	Editor	Fortune Magazine
Tango Matsumoto	Corporate Executive Officer; Senior Vice-President; Head, Global Marketing	Fujitsu Limited
Jody Westby	Chief Executive Officer	Global Cyber Risk
Christy Wyatt	Chief Executive Officer	Good Technology
Nicko van Someren	Chief Technology Officer	Good Technology
Jacob West	Chief Technology Officer, Enterprise Security Services	Hewlett-Packard Company
Mike Nefkens	Executive Vice-President & General Manager, Enterprise Services	Hewlett-Packard Company
John Flint	Managing Director	HSBC Holdings Plc
Paul Thierney	Global Head, Technology Services	HSBC Holdings Plc
Geoff Bickers	Director, Cyber Security	Internet Corporation for Assigned Names and Numbers (ICANN)
Patrick Jones	Senior Director, Global Stakeholder Alliances	Internet Corporation for Assigned Names and Numbers (ICANN)
Larry Clinton	President and Chief Executive Officer	Internet Security Alliance
Adam Firestone	President	Kaspersky Government Solutions
Adam Golodner	Partner, Leader Global Cybersecurity & Privacy Group	Kaye Scholer LLP
Christophe Nicolas	Senior Vice-President and Head, Kudelski Security	Kudelski Group
Jean-Philippe Aumasson	Principal	Kudelski Group
Martin Dion	Vice President, Head of Financial Services Practices	Kudelski Group
Andres Ruzo	Chief Executive Officer	Link America

Haden Land	Vice President, Research & Technology	Lockheed Martin Corporation
Kevin Mahaffey	Co-Founder & Chief Technology Officer	Lookout Mobile Security
Stefano Orsini	Head of Information Security and Risk	Luxottica
Peter Beshar	General Counsel, Executive Vice-President	Marsh & McLennan Companies
Preston McAfee	Corporate Vice-President and Chief Economist	Microsoft Corporation
Brian Behlendorf	Managing Director	Mithril Capital Management
Daniel Prieto	Director, Cybersecurity, Privacy and Civil Liberties	National Security Council
General Dick Berlijn	Retired Royal Netherlands Air Force four-star general former Chief of Defence of the Netherlands	Netherlands
Aditya Fotedar	Chief Technology Officer	Nexenta
Jon Bruner	Editor at Large	O'Reilly Media
Belisario Conreras	Program Manager, Cyber Security	Organization for American States
Eric Rosenblum	Forward Deployed Engineer	Palantir Technologies
Melody Hildebrandt	Global Cyber Security Lead	Palantir Technologies
David Broadhead	Group Information Security Manager & Head of High Technology Investigations	Prudential Plc
Burke Norton	Chief Legal Officer	Salesforce
Peter Schwartz	Senior Vice-President, Global Government Relations and Strategic Planning	Salesforce
Rod Beckstrom	Chief Security Advisor	Samsung Electronics Co. Ltd
Gerold Huebner	Chief Product Security Officer	SAP SE
Ben Krutzen	Information Risk Management	Royal Dutch Shell Plc
Marc Goodman	Chair for Policy and Law	Singularity University
Jan Verplancke	Director, Chief Information Officer and Group Head, Technology and Operations	Standard Chartered Bank
Kirstjen Nielsen	President	Sunesis Consulting
Rajiv Pant	Chief Technology Officer	The New York Times
Annemarie Zielstra	Director International Relations	TNO
Alberto Yepez	Managing Director	Trident Capital
John Villasenor	Professor	University of California Los Angeles
Hans Brechbuhl	Executive Director, Center for Digital Strategies	University of Dartmouth
Ellen Richey	Chief Enterprise Risk Officer	Visa Inc
Robert Vamosi	Author	When Gadgets Betray Us
Guha Ramasubramanian	Head, Office of the CEO	Wipro Limited
Ken Hall	Vice-President, Cyber Security	Wipro Limited
Francis Bouchard	Group Head of Government and IndustryAffairs	Zurich Insurance Group
Jeremy Smith	Head of Technology	Zurich Insurance Group

Project Team

World Economic Forum

Alan Marcus	Senior Director, Head of Information and Communication Technology Industries
Derek O'Halloran	Director, Head of Information Technology Industry
Elena Kvochko	Manager, Information Technology Industry, Partnering for Cyber Resilience

Deloitte

Jacques Buith	Managing Partner, Risk Services
Dana Spataru	World Economic Forum Project Manager

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum is an international institution committed to improving the state of the world through public-private cooperation in the spirit of global citizenship. It engages with business, political, academic and other leaders of society to shape global, regional and industry agendas.

Incorporated as a not-for-profit foundation in 1971 and headquartered in Geneva, Switzerland, the Forum is independent, impartial and not tied to any interests. It cooperates closely with all leading international organizations.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org